BY ORDER OF THE COMMANDER
AIR RESERVE PERSONNEL CENTER

ARPC INSTRUCTION 33-1120
29 NOVEMBER 2001

Operations

MOBILE COMPUTING, ISSUES AND RETURNS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR:HQ ARPC/SCMH
(Leendert H. Stuyt)

Certified by: HQ ARPC/SCM (Lt Col F.Bromley III)
Pages: 4
Distribution: F

This publication implements policies, responsibilities, and procedures for requesting and using mobile computing devices (also known as notebooks, laptops, and handhelds, Personal Digital Assistants (PDAs), i.e., Blackberry, 3COM Notepad, IBM Workpad etc. It covers general guidance and responsibilities for the correct management of mobile computing throughout its life cycle.

1. Authorized Mobile Computing Devices (MCDs). All computing systems connected to any local network must be protected by anti-virus programs to prevent proliferation of virus and worm type infections of other computer systems and must be authorized. All government issued computer systems are authorized, but must be equipped with current and appropriate anti-virus programs as directed by Information Protection (SCMD). Personally owned personal digital assistants may be authorized as determined by the Designated Approval Authority (DAA). However, to date, no Department of Defense (DoD) approved software exists that can detect, erase or prevent virus infection of personal digital assistants. Until such time that virus detecting tools are available, all personal digital assistants will be prohibited from connecting to the Air Reserve Personnel Center's (ARPC) network. When appropriate software becomes available, SCMD will issue guidance on its use and the connection of personal digital assistant's to the ARPC network.

2. Responsibilities and Authorities.

2.1. Helpdesk (SCMH). SCMH is responsible for programming and management of MCDs, and is the sole responsible agency for configuring and maintaining these devices. Some of the names used are: Notebooks, laptops, hand held, small computing devices, and Black Berries (this list is not inclusive). A definition is any device that can provide the user with the ability to perform their job on an MCD away from their normal duty station (i.e., assigned desk area with standard CPU). Final issuance authority for all MCDs is the Helpdesk. The Helpdesk maintains a data base that list all current active notebooks, laptops, handheld devices or any other device that can be issued based on the above stated criteria. Copies are maintained by the Helpdesk while the request is active. Weekly reports are provided to Network Operations (SCMN) to track Remote Access Services (RAS) access. To whom the MCD is signed out OK and then the list is retired per AFI (filing authority).

2.2. Issuing MCDs. MCDs may be issued to persons going TDY or with a recurring need for the device. SCMH will issue MCDs as set out in paragraph 2.2.2.

2.2.1 Directorate MCDs. Some directorates have their own MCDs and may issue these devices in accordance with directorate policy. Such a device shall be issued using an AF Form 1297, **Temporary Issue Receipt**, signed by the primary or alternate Automatic Data Processing Equipment (ADPE) custodian of the account with the MCD.

2.2.2 Requester. Requester is defined as any person who is authorized to request an MCD for temporary duty or other authorized absence away from the assigned desk area requiring the ability to perform their daily duties on the MCD. Current established procedure is for the user to request mobile computing support by sending an e-mail to: ARPC.LAPTOP@arpc.denver.af.mil. Request can be mailed both internally (inside ARPC's domain) and externally (anywhere from the planet) to this address. The requester will receive an acknowledgement of receipt and if there are any other questions, they will be contacted. ARPC Form 78, **Mobile Computing Device (MCD) Request,** must be filled out on the INTRANET or with FormFlow and forwarded to the above e-mail location for processing. The form can either be in paper or electronic format.

2.3. Directors. Directors in ARPC are required to approve the ARPC Form 78 for Remote Access Services (RAS), which requires remote access to ARPC's Local Area Network Domain.

2.4. DAA. After RAS is requested and approved by the requestor's director, the DAA, in ARPC the Director of SC, also approves access to the LAN.

2.5. Information Protection (SCMD). SCMD will monitor RAS access and discontinue after expiration date of request if not discontinued already. A copy of ARPC Form 78 is provided to track RAS access. SCMD's coordination on ARPC Form 78 is not needed.

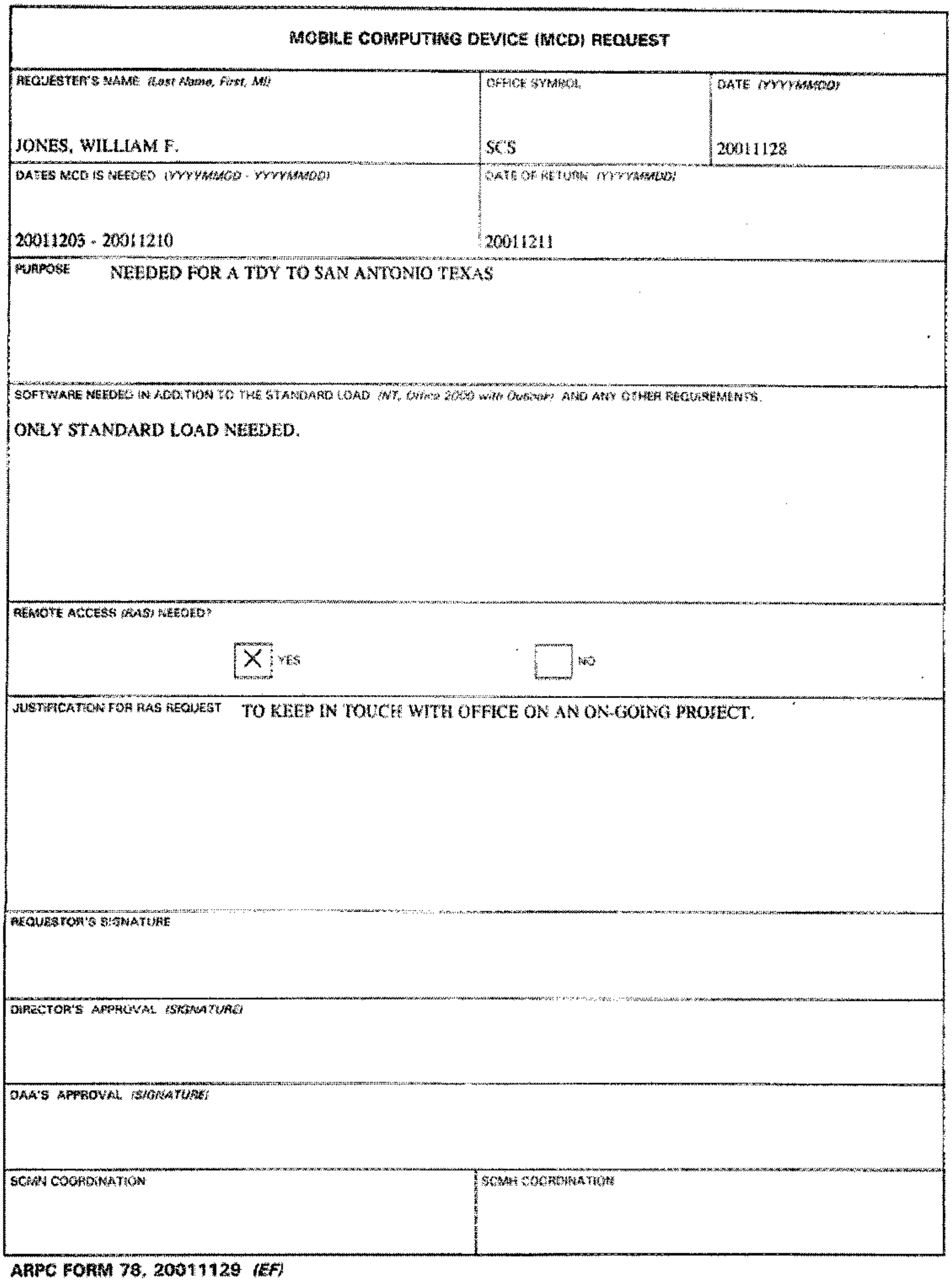
2.6 Network Control Center (SCMN). SCMN verifies the authenticity of the requestor (valid LAN account), maintains a list of active MCD users with current RAS access and will notify Helpdesk when the suspense date is expired on RAS and turned off.

3. Form Prescribed. ARPC Form 78.

Kirk A. Jamison
Chief, Systems Services Division
Directorate of Communications
and Information

ATTACHMENT 1—ARPC FORM 78

ATTACHMENT 1
ARPC FORM 78



MOBILE COMPUTING DEVICE (MCD) REQUEST

REQUESTER'S NAME *(Last Name, First, MI)* JONES, WILLIAM F.	OFFICE SYMBOL SCS	DATE *(YYYYMMDD)* 20011128
DATES MCD IS NEEDED *(YYYYMMDD - YYYYMMDD)* 20011205 - 20011210	DATE OF RETURN *(YYYYMMDD)* 20011211	

PURPOSE NEEDED FOR A TDY TO SAN ANTONIO TEXAS

SOFTWARE NEEDED IN ADDITION TO THE STANDARD LOAD *(NT, Office 2000 with Outlook)* AND ANY OTHER REQUIREMENTS.

ONLY STANDARD LOAD NEEDED.

REMOTE ACCESS *(RAS)* NEEDED?

☒ YES ☐ NO

JUSTIFICATION FOR RAS REQUEST TO KEEP IN TOUCH WITH OFFICE ON AN ON-GOING PROJECT.

REQUESTOR'S SIGNATURE

DIRECTOR'S APPROVAL *(SIGNATURE)*

DAA'S APPROVAL *(SIGNATURE)*

SCMN COORDINATION	SCMH COORDINATION

ARPC FORM 78, 20011129 *(EF)*